Duration: 60 min | Amazon Web Services | Solutions Architect | IAM

Identity Access Management - IAM

Amazon Web Services

IAM

Introduction

- IAM is a web service that helps you securely control access to AWS resources.

- To manage users and their level of access to the AWS Console

- IAM is a Global Service, It doesn’t Apply to regions.

- IAM Allows you to create

    1. Users
    2. Groups
    3. Policies
    4. Roles

Features

- Shared Access to your AWS Account
- Granular Permissions
- Multi Factor Authentication
- Own Password Policies
- Identity Federation
- Supports PCI DSS Compliance

Root User

- Root Account is the account created, when we setup our AWS Account
- Owner of our AWS Account
- It has Complete Admin Access
- Amazon recommend to not to use Root account for day to day activities

IAM User

- IAM users are not separate accounts; they are users within your account.

- Own individual username & Password

- IAM User Access Types

    1. AWS Management Console Access
    2. Programmatic Acccess

- By default, New user will get No Permissions

AWS Management Console Access type

1. Can login to AWS Account using Browser

2. Will Get Username & Password

Programatic Access Type

1. Can Login to AWS Account using CLI, SDK or API

2. Will get Access Key ID & Secret Access Key

Groups

- Collection of Identical Users
- Users will inherit the Permissions from the Group

Policies

- Policies are made up of Documents, Which contains the Permission statements
- Policies are written in JSON Format
- Polices Can be attached to Users & Groups

Roles

- Role is an Identity With the Permission Policies
- Roles Can be used to apply permissions to Resources

To DO List

1. Activate MFA on AWS Account

2. Create a Password Policy With the below options.

    a) Min Password Length – 10 Characters
    b) UpperCase Letters
    c) Lower Case Letters
    d) Numbers
    e) Special Characters
    f) Password history – 3
    g) Password age – 45 Days